DSP-Explorer Managed Service Monitoring Setup Requirements

DSP-Explorer Managed Service - Key Monitoring Pre-Requisites

The key items required to configure our monitoring product are detailed below for your reference.

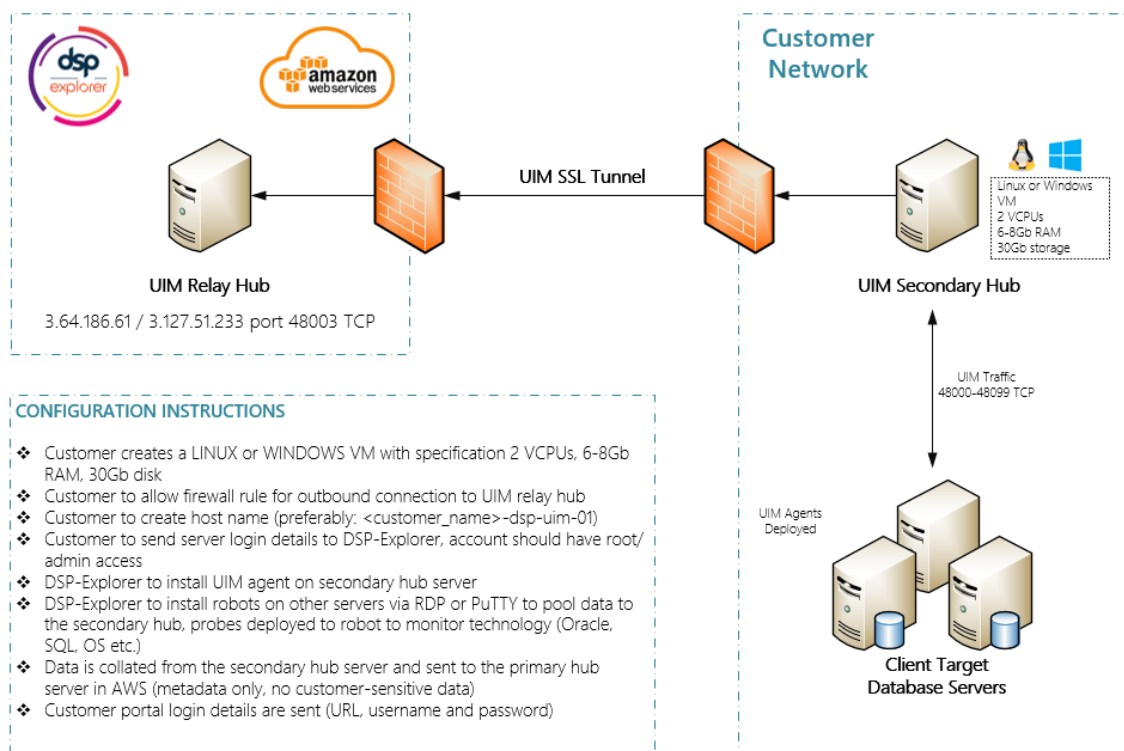1. A small monitoring hub inside your network is required, additional details can be found below.

The server can be either a Windows or Linux server (Centos, Red Hat, SLES) with the following spec when using a hypervisor to provision.

- 2 VCPUs
- 6 – 8Gb RAM
- 30Gb disk space

In terms of the network requirements and general layout of the monitoring, hopefully, the picture below will help. The main communication points are listed below in case the picture is not clear.

- Bi-Directional communication is required between the hub and all servers over ports 48000 – 48099
- Outgoing communication is required between the hub and our master hub (3.64.186.61 [3.127.51.233 is backup]) over port 48003
- Root / Admin access is required to install the robot (small agent) onto each monitored server
- Root / Admin access is required to the hubs to install the required software and configuration.

Customer UIM Hub Topology

Customer Network

UIM SSL Tunnel

Linux or Windows VM
2 VCPUs
6-8Gb RAM
30Gb storage

UIM Relay Hub

3.64.186.61 / 3.127.51.233 port 48003 TCP

UIM Secondary Hub

UIM Traffic
48000-48099 TCP

UIM Agents Deployed

Client Target Database Servers

CONFIGURATION INSTRUCTIONS

- ❖ Customer creates a LINUX or WINDOWS VM with specification 2 VCPUs, 6-8Gb RAM, 30Gb disk
- ❖ Customer to allow firewall rule for outbound connection to UIM relay hub
- ❖ Customer to create host name (preferably: <customer_name>-dsp-uim-01)
- ❖ Customer to send server login details to DSP-Explorer, account should have root/ admin access
- ❖ DSP-Explorer to install UIM agent on secondary hub server
- ❖ DSP-Explorer to install robots on other servers via RDP or PuTTY to pool data to the secondary hub, probes deployed to robot to monitor technology (Oracle, SQL, OS etc.)
- ❖ Data is collated from the secondary hub server and sent to the primary hub server in AWS (metadata only, no customer-sensitive data)
- ❖ Customer portal login details are sent (URL, username and password)